City and County of San Francisco

Committee on Information Technology

Regular Meeting

November 16, 2023

Meeting Broadcast & Public Comment

- Today's meeting will be broadcast live via WebEx. Link can be found on the COIT website at sf.gov/COIT
- Public commenters who are participating remotely can join the WebEx or call 415-655-0001 and use access code 2664 566 1417, webinar password COIT (2648 from video systems).
- To speak when public comment is open, dial *3 or use the WebEx raise hand feature.

Agenda

1. Call to Order by Chair
2. Roll Call
3. General Public Comment
4. Approval of the Meeting Minutes from September 21, 2023 (Action Item)
5. Review Surveillance Technology Policy - Police Department - Drone or Unmanned Aerial Systems (Action Item)
6. Review Surveillance Technology Policy Amendments - City Administrator's Office - Security Cameras (Action Item)
7. Update on Generative AI Planning
8. Chair Update
9. CIO Update
10. Adjournment

Item Number 3

General Public Comment

Item Number 4

Approval of the Meeting Minutes from September 21, 2023

Action Item

Item Number 5

Review Surveillance Technology Policy - Police Department - Drone or Unmanned Aerial Systems

Action Item

City and County of San Francisco

Police Department

Unmanned Aerial Systems (UAS)

November 16, 2023

Authorized Use Cases

Aerial perspective during the following specified uses:

- Sideshows (AKA stunt driving) and/or street takeover events where many vehicles and reckless driving are present.
- Major and Critical incidents as defined by SFPD General Order 8.01, including but limited to mass casualty events, natural disasters or Hazardous material incidents.
- High-risk search warrant service.
- Apprehension of armed and dangerous and/or violent suspects.
- Hostage/Crisis Negotiations Team (H/CNT) incidents.

Authorized Use Cases, continued:

- Pre-planned deployment mapping.
- Search & rescue operations.
- Post-incident crime scene mapping, preservation, and documentation.
- Apprehension of suspects who have fled on foot.
- Auto Burglary and Robbery Abatement Operations.
- When there is probable cause to arrest or reasonable suspicion to detain an occupant of a vehicle and reasonable belief that the operator of the vehicle is likely to flee if a vehicle stop is attempted.
- Department training relating to authorized uses.

Technology Description

Generally, a UAS consists of:

- Chassis with several propellers for flight
- Control propellers and other flight stabilization technology
- Radio frequency and antenna equipment to communicate with remote-control unit
- A camera
- Audio recording
- A digital image/video storage system for recording into a digital data memory card
- A remote-control unit
- Battery charging equipment for the aircraft and remote control

Requirements and Considerations

- FAA Remote Pilot Certification
- FAA Certificate of Authorization
- First Responder Tactical Beyond Visual Line of Sight (TBVLOS) Waiver
- Standard reporting of UAS logs
- Overlap with Assembly Bill 481, requiring BOS annual review

Data Lifecycle Summarized

Type of Data Collected: Still images, thermal imaging and/or video.

Who Has Access To That Data: Non-sworn members with authorization from Chief of Police, or designee; Authorized sworn members designated and trained as UAS Operators and Administrators; Q2 Police Officers- 0390 Chief of Police; Legal staff

Data Lifecycle Summarized

Who Data is Shared With Outside of Dept: DA's Office; Public Defender's Office (via DA's Office in accordance with discovery laws); Law enforcement partners; Parties to civil or criminal litigation, or other third parties, in response to a valid Defense Subpoena; DPA; Media outlets.

How Long Data is Retained: Min of 60 days.

How is Data Disposed: Deleting/wiping/erasing/degaussing or otherwise make data irretrievable.

PSAB Suggested Edits

- Force option prohibition
- Clarify whether data wll be redacted (PRA/Media release)
- Limit recording footage to on-scene only
- Internal periodic and random audits including GPS data (if available)
- Vendor neutral language
- Clarify definition of pre-planned deployment mapping

PSAB Meeting Dates

- August 24, 2023, and November 7, 2023
- PSAB recommends approval.

Questions

Item Number 6

Review Surveillance Technology Policy Amendments - City Administrator's Office - Security Cameras

Action Item

City and County of San Francisco

Office of the City Administrator

Surveillance Technology Policy Amendments

November 16, 2023

Technology Description

The Security Camera System (fixed or mobile) will be used to support operations of the Office of the City Administrator (CAO) and the divisions/departments (referred to as CAO agencies) under its control.

The proposed policy is a modification of the existing policy that governs the Real Estate Division*

Summary of Amendments

- Create a policy that applies to all agencies with the Office of the City Administrator, including Treasure Island Development Authority (TIDA); TIDA is not covered under the current policy focused on the Real Estate Division (RED);
- Amend the existing policy to allow certain Animal Care and Control (ACC) staff to monitor live and review recorded footage without the approval of the RED Director; and
- Allow the acquisition of cameras in the future without needing to create/amend the policy.

Proposed Amendment: CAO-wide Policy

- Current policy applies to surveillance cameras used in or around assets in the RED portfolio.
- Amended policy would apply to all CAO agencies, and surveillance cameras used in or around assets in the portfolio of any of its divisions, including TIDA.

*****The policy will still largely rely on RED for implementation: RED controls 511 of 516 cameras within the CAO portfolio.*****

Proposed Amendment: Why add TIDA?

- Treasure Island Ferry Terminal acquisition in early 2024;
- Ferry Terminal has 5 security cameras (Avigilon);
- Add TIDA staff, lessees (TICD) and contractors to the policy to access data from security cameras (live, reviewing recordings and exporting data)

Proposed Amendment: Animal Care & Control

- Current policy:
  - Only allows security to monitor live feed;
  - requires the RED Director's approval before reviewing recorded video
- Proposed amendments:
  - Allow specific ACC staff to monitor live and review recorded video under certain circumstances to better respond to issues as they arise.
  - Note that the export process remains unchanged.

Proposed Amendment: Acquisition of Future Cameras

- Allow the acquisition of cameras in the future without requiring a policy amendment. Future cameras would be included in the annual surveillance inventory.

Authorized Use Cases (No changes)

1. Live monitoring.
2. Recording of video and images.
3. Reviewing camera footage in the event of an incident.
4. Providing video footage/images to law enforcement or other authorized persons following an incident or upon request.

Other Details as needed

- In large part, the proposed amendments do not alter the fundamental structure of the existing RED policy.
- The proposed amendments are intended to provide expanded access to surveillance video to certain ACC staff; and,
- The proposed amendments are intended to extend the existing policy to include buildings and assets outside of the RED portfolio, including TIDA assets.

PSAB Meeting Dates

- November 7, 2023
- PSAB recommends approval.

Questions

Item Number 7

Update on Generative AI Planning

Discussion Item

San Francisco Office of the City Administrator

Generative AI Guidelines

Committee on Information Technology

November 16, 2023

Agenda

- Definitions
- Guidelines
  - Do's
  - Don’ts
- Role of IT Leaders
- Next Steps

Definitions

Guidelines

- Do's
- Don’ts

Role of IT Leaders

Next Steps

What do we mean when we say AI?

Artificial Intelligence (AI) is a broad category of technology with great potential to provide public benefits, when used responsibly.

Generative AI is distinct from Discriminative Machine Learning models which have been widely used since the early 2000s, including by the City. DML models do not generate new content; they are limited to generating known and validated values.

Examples:

- 311 app's photo recognition to help users classify their report type
- ASR's ML appraisal system to predict real estate prices and identify re-appraisal targets

What about Generative AI?

Generative AI technology generates new data based on patterns learned from existing data and can produce content that mimics human creativity. Examples include text generation, image creation, and music_composition. These tools use machine learning algorithms that have been trained on very large sets of text and image data culled from the internet (which often contain gender, racial, political, and other biases).

Generative AI differs from AI technology currently in use by the City, which supports informed decisions based on input data but does not create new content.

Common Applications:

- ChatGPT
- Bard
- Dall-E
- Midjourney

Risks of Generative AI

Generative AI excels at producing content that appears authoritative and polished, making it easy to accept AI-generated content at face value. Risks include:

- Producing inaccurate information, either to the public or to City staff
- Inaccurately attributing AI-generated content to official SF sources
- Making a decision based on inaccurate AI-generated content that negatively affects residents
- Cybersecurity problems or other errors due to the use of AI-generated code
- Exposing non-public data when entering a prompt (most prompts become part of training data sets)

Definitions

Guidelines

- **Do's**
- **Don’ts**

Role of IT Leaders

Next Steps

Three key guidelines

- **ALWAYS** review and fact check AI-generated content before using it.
- **ALWAYS** disclose usage of Generative AI in your output.
- **NEVER** enter sensitive information into public generative AI tools (such as ChatGPT); this information can be viewed by the companies that make the tools and, in some cases, by other members of the public.
  Please refer to Citywide Data Classification Standard for more specifics on data classification and department responsible roles.

DO’s of Generative AI

- **Try it out!** Experiment with Generative AI tools for drafting, leveling, and formatting text and explanatory images using public information.
- Work with your department IT team and experiment thoroughly with various use cases before using generative AI in the delivery of programs or services.
- Thoroughly **review and fact check** all AI-generated content (e.g. text, code, images, etc). You are responsible for what you create with generative AI assistance.
- Disclose when and how generative AI was used in your work.

  “The header image was created using the AI tool MidJourney”

  “This abstract was created using Bard, a generative AI tool”

  “FYI, I used ChatGPT to revise this email”

DON’Ts of Generative AI

- **Don't enter** into public generative AI tools (e.g. ChatGPT) any information that cannot be fully released to the public.
- **Don't publish** generative AI output (whether text, image, or code) without full knowledgeable review and disclosure.
- **Don't ask** Generative AI tools to find facts or make decisions without expert human review.
- **Don't conceal** use of Generative AI during interaction with colleagues or the public, such as tools that may be listening and transcribing the conversation or tools that provide simultaneous translation.

DON’Ts continued

- **Don't generate** images, audio, or video that could be mistaken for real people, such as:
  - Making a fake photo or recording of a specific San Francisco official or member of the public (“deepfake”) - even with disclosure
  - Generating a fake image or recording that purports to be a San Franciscan or public official, even if not a specific one
  - Generating fake “respondents” or made-up profiles for surveys or other research

Definitions

Guidelines

- Do's
- Don’ts

Role of IT Leaders

Next Steps

For IT leaders (general)

- Disseminate guidelines across your department.
- Begin collecting use cases and be prepared to report your uses in a public forum to ensure transparency and accountability.
- Know whether software you manage - and its components - include Generative AI; inform your team how it is used and what the specific risks are.
- Ask questions about Generative AI in your procurement solicitations.
- Work with vendors to ensure that AI built into procured tools will be explainable and auditable. Vendors should be able to provide information and documentation on data sources, methods, and validation.

For IT leaders (specific)

- Experiment with training internal models on internal data.
- Consult with the Office of Cybersecurity before developing and/or purchasing Generative AI technologies.
- When considering implementing chatbots for service to the public, thoroughly test and develop a language access plan.

Definitions

Guidelines

- Do's
- Don’ts

Role of IT Leaders

Next Steps

2024 – Next Steps

1. **Guideline Distribution**

   CAO will work with department staff to ensure Gen AI guidelines are widely accessible and understandable

2. **Baselining & Research**

   MYR, CAO, and DT coordinate to identify and catalog **existing** AI technology use, and **emerging** use cases

3. **Stakeholders & Public Engagement**

   MYR + CAO to develop public engagement plan, including academic experts, SF residents, and industry

4. **Ethical Use & Governance Framework**

   CAO + MYR develop ethical use principles to evaluate future tech opportunities

5. **Training & Procurement**

   CAO + DT develop staff training & procurement processes

Questions and comments?

Thank You!

Item Number 8

Chair Update

Item Number 9

CIO Update

Adjournment